CLAIMS

We claim:

1. A method of operating an intrusion detection system according to a business rule, comprising the steps of:

awaiting an update time of the intrusion detection system;

responsive to occurrence of an update time, checking a validity condition of a business rule to determine whether a provision of the business rule is a newly operative provision;

if the provision of the business rule is a newly operative provision, altering an intrusion set according to the newly operative provision.

2. The method of claim 1, wherein the validity condition is a temporal validity condition.

3. The method of claim 1, wherein the validity condition is a network validity condition.

4. The method of claim 1, wherein the validity condition is a compound validity condition.

5. A method of operating an intrusion detection system according to a set of business rules, comprising the steps of:

awaiting an update time of the intrusion detection system;

responsive to occurrence of an update time, checking validity conditions of a plurality of business rules to determine whether a provision of any of the plurality of business rules is a newly operative provision;

for each provision of the plurality of business rules that is a newly operative provision, altering an intrusion set according to the newly operative provision.

6. The method of claim 5, wherein the validity condition is a temporal validity condition.

7. The method of claim 5, wherein the validity condition is a network validity condition.

8. The method of claim 5, wherein the validity condition is a compound validity condition.

9. A method of operating an intrusion detection system according to a set of business rules, comprising the steps of:

awaiting an update time of the intrusion detection system;

responsive to occurrence of an update time, checking validity conditions of the set of business rules to determine whether a provision of any of the set of business rules is a newly operative provision;

for each newly operative provision, checking an intrusion set to determine whether the newly operative provision applies to the intrusion set; and

if the new provision applies to the intrusion set, altering the intrusion set according to the newly operative provision.

10. The method of claim 9, wherein the validity condition is a temporal validity condition.

11. The method of claim 9, wherein the validity condition is a network validity condition.

12. The method of claim 9, wherein the validity condition is a compound validity condition.

13. The method of claim 9, wherein the step of altering the intrusion set includes the step of altering a signature of the intrusion set.

14. The method of claim 9, wherein the step of altering the intrusion set includes the step of altering a threshold of the intrusion set.

15. The method of claim 9, wherein the step of altering the intrusion set includes the step of altering an action of the intrusion set.

16. The method of claim 9, wherein the step of altering the intrusion set includes the step of altering a weight of the intrusion set.

17. The method of claim 9, wherein the update time is a scheduled time.

18. The method of claim 9, wherein the update time is one of a plurality of update times that occur substantially periodically.

19. The method of claim 9, wherein the update time is a computed update time.

20. The method of claim 9, wherein the set of business rules includes exactly one individual rule.

21. The method of claim 9, wherein the set of business rules includes more than one individual rule.